IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Oleg Zaboronski et al.	Examiner:	Unknown
Serial No.:	10/027,237	Group Art Unit:	2819
Filed:	December 20, 2001	Docket:	1365.059US1
Title:	LOGIC CIRCUITS FOR PERFORMING MODULAR MULTIPLICATION AND EXPONENTIATION		

INFORMATION DISCLOSURE STATEMENT

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In compliance with the duty imposed by 37 C.F.R. § 1.56, and in accordance with 37 C.F.R. §§ 1.97 *et. seq.*, the enclosed materials are brought to the attention of the Examiner for consideration in connection with the above-identified patent application. Applicants respectfully request that this Information Disclosure Statement be entered and the documents listed on the attached Form 1449 be considered by the Examiner and made of record. Pursuant to the provisions of MPEP 609, Applicants request that a copy of the 1449 form, initialed as being considered by the Examiner, be returned to the Applicants with the next official communication.

Pursuant to 37 C.F.R. §1.97(b), it is believed that no fee or statement is required with the Information Disclosure Statement. However, any fee deemed to be due may be charged to Deposit Account No. 19-0743 in order to have this Information Disclosure Statement considered.

Pursuant to 37 C.F.R. 1.98(a)(2), Applicant believes that copies of cited U.S. Patents and Published Applications are no longer required to be provided to the Office. Notification of this change was provided in the United States Patent and Trademark Office OG Notices dated October 12, 2004. Thus, Applicant has not included copies of any US Patents or Published Applications cited with this submission. Should the Office require copies to be provided, Applicant respectfully requests that notice of such requirement be directed to Applicant's below-signed representative. Applicant acknowledges the requirement to submit copies of foreign patent documents and non-patent literature in accordance with 37 C.F.R. 1.98(a)(2).

The Examiner is invited to contact the Applicants' Representative at the below-listed telephone number if there are any questions regarding this communication.

Respectfully submitted,

OLEG ZABORONSKI ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 349-9587

Date 17 June '05 By _____
Timothy B Clise
Reg. No. 40,957

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 17th day of June, 2005.

CANDIS BUENDING
Name

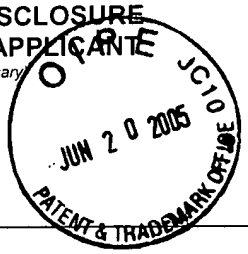
_____
Signature

PTO/SB/08A(10-01)
Approved for use through 10/31/2002. OMB 651-0031
US Patent & Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known	
Application Number	10/027,237
Filing Date	December 20, 2001
First Named Inventor	Zaboronski, Oleg
Group Art Unit	2819
Examiner Name	Unknown

Sheet 1 of 3

Attorney Docket No: 1365.059US1

US PATENT DOCUMENTS

Examiner Initial *	USP Document Number	Publication Date	Name of Patentee or Applicant of cited Document	Filing Date If Appropriate
	US-2002/0026465 A1	02/28/2002	Rumynin, D., et al.	01/25/2001
	US-2002/0078110 A1	06/20/2002	Rumynin, D., et al.	07/27/2001
	US-2004/0153490 A1	08/05/2004	Talwar, S., et al.	11/14/2003
	US-4,399,517	08/16/1983	Niehaus, Jeffrey A., et al.	03/19/1981
	US-5,187,679	02/16/1993	Vassiliadis, Stamatis , et al.	06/05/1991
	US-5,321,752	06/14/1994	Iwamura, K., et al.	09/04/1992
	US-5,325,320	06/28/1994	Chiu, Chiao-Er A.	05/01/1992
	US-5,343,417	08/30/1994	Flora, Laurence P.	11/20/1992
	US-5,497,342	03/05/1996	Mou, Z.-J. , et al.	11/09/1994
	US-5,524,082	06/04/1996	Horstmann, P., et al.	06/28/1991
	US-5,701,504	12/23/1997	Timko, M. A.	12/28/1994
	US-5,964,827	10/12/1999	Ngo, H. C., et al.	11/17/1997
	US-6,023,566	02/08/2000	Belkhale, K., et al.	04/14/1997
	US-6,175,852	01/16/2001	Dhong, S. H., et al.	07/13/1998
	US-6,269,386	07/31/2001	Siers, S. E., et al.	10/14/1998
	US-6,490,608	12/03/2002	Zhu, Jay	12/09/1999

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	T[2]
	EP-0168650A2	01/22/1986	Darringer, J., et al.	
	EP-0309292A2	03/29/1989	Nishiyama, T., et al.	
	EP-0442356A2	08/21/1991	Chang, Y. C.	
	EP-0947914A1	10/06/1999	McGregor, M. S.	
	GB-2263002	07/07/1993	Poon, J. T.	
	GB-2318892	05/06/1998	Hobson, R. D., et al.	
	WO-99/22292A1	05/06/1999	Verbauwhede, I.	
	WO-03/052583A2	06/26/2003	Meulemans, P., et al.	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

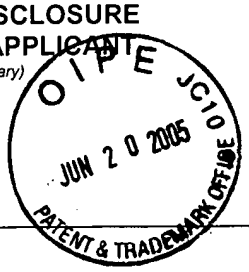
Examiner Initials*	Cite No [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		"PCT international Search Report relating to PCT/GB 03/05489", (September 15, 2004), 4 pgs.	

EXAMINER **DATE CONSIDERED**

Substitute Disclosure Statement Form (PTO-1449)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

Substitute for form 1449A/PTO
INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)



Complete if Known	
Application Number	10/027,237
Filing Date	December 20, 2001
First Named Inventor	Zaboronski, Oleg
Group Art Unit	2819
Examiner Name	Unknown

Sheet 2 of 3

Attorney Docket No: 1365.059US1

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	**Cite No [1]**	**Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.**	**T[2]**
		"United Kingdom Search Report relating to Great Britain Patent Application No. GB 0130255.3", (June 20, 2002), 1 pg.	
		"United Kingdom Search Report relating to Great Britain Patent Application No. GB0326611.1", (March 29, 2004), 1 pg.	
		BEDRIJ, O. J., "Carry-Select Adder", IRE Trans., EC-11, (June 1962), 340-346	
		BOOTH, A., "A Signed Binary Multiplication Technique", Oxford University Press, Reprinted from Q.J. Mech. Appl. Math. 4:236-240,(1951), 100-104	
		CHAKRABORTY, S., et al., "Synthesis of Symmetric Functions for Path-Delay Fault Testability", 12th International Conference on VLSI Design, (1999), 512-517	
		DADDA, L., "On Parallel Digital Multipliers", Associazione Elettrontecnia ed Elettronica Italiana, Reprinted from Alta Freq. 45:574-580,(1976), 126-132	
		DADDA, L., "Some Schemes For Parallel Multipliers", Assocciazione Elettrotenica ed Elettronica Italiana, Reprinted from Alta Freq. 34:349-356,(1965),Pgs. 118-125	
		DEBNATH, D., "Minimization of AND-OR-EXOR Three-Level Networks with AND Gate Sharing", IEICE Trans. Inf. & Syst., E80-D, 10, (1997),pp. 1001-1008	
		DRECHSLER, R., et al., "Sym*pathy*: Fast Exact Minimization of Fixed Polarity Reed-Muller Expressions for Symmetric Functions", IEEE ED&TC 1995, Proceedings European Design and Test Conference, (March 6-9, 1995), 91-97	
		ELDRIDGE, S. E., et al., "Hardware Implementation of Montgomery's Modular Multiplication Algorithm", IEEE Transactions on Computers, 42(6), (1993), 693-699	
		FOSTER, C., et al., "Counting Responders in an Associative Memory", The Institute of Electrical and Electronics Engineers, Inc., Reprinted, with permission, from IEEE Trans. Comput. C-20:1580-1583,(1971), 86-89	
		FREKING, W. L., et al., "Parallel Modular Multiplication With Application to VLSI RSA Implementation", Proceedings of 1999 the IEEE International Symposium on Circuits and Systems, Vol. 1, (1999), 490-495	
		GOTO, G., et al., "A 54 x 54-b Regularly Structured Tree Multiplier", IEEE Journal of Solid-State Circuits, Vol 27, No. 9, (Sept. 1992), 1229-1236	
		HEKSTRA, G. J., et al., "A Fast Parallel Multiplier Architecture", IEEE International Symposium on Circuits and Systems; Institute of Electrical and Electronic Engineers, c1977-c1996, 20v. :ill. :28cm, (1992), 2128-2131	
		KNOWLES, S., "A Family of Adders", Proc. 14th IEEE Symp. on Computer Arithmetic, (1999),30-34	
		KOGGE, P. M., et al., "A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations", IEEE Trans. Computers, Vol. C-22, No. 8, (Aug. 1973), 786-793	
		LADNER, R. E., et al., "Parallel Prefix Computation", Journal of ACM, Vol. 27, No. 4, (Oct. 1980), 831-838	

EXAMINER **DATE CONSIDERED**

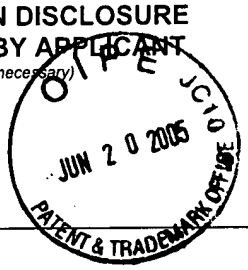
* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional) [2] Applicant is to place a check mark here if English language Translation is attached

PTO/SB/08A(10-01)
Approved for use through 10/31/2002. OMB 651-0031
US Patent & Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known	
Application Number	10/027,237
Filing Date	December 20, 2001
First Named Inventor	Zaboronski, Oleg
Group Art Unit	2819
Examiner Name	Unknown

Sheet 3 of 3

Attorney Docket No: 1365.059US1

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		LING, H., "High-Speed Binary Adder", IBM Journal of Research and Development, Vol. 25, No. 3, (1981), 156-166	
		MARNANE, W. P., "Optimised Bit Serial Modular Multipler for Implementation on Field Programmable Gate Arrays", Electronics Letters, 34(8), (1998), 738-739	
		NICHOLSON, J. O., "Parallel-Carry Adders Listing Two-Bit Covers", IBM Technical Disclosure Bulletin, 22(11), (April, 1980),5036-5037	
		NIENHAUS, H. , "Efficient Multiplexer Realizations of Symmetric Functions", IEEE, (1981), 522-525	
		OKLOBDZIJA, V G., et al., "Improving multiplier design by using improved column compression tree and optimized final adder in CMOS technology", IEEE transactions on Very Large Scale Integration (VLSI) Systems, IEEE, Inc, New York, vol. 3, no. 2,(1995), 292-301	
		ONG, S., et al., "A Comparison of ALU Structures for VLSI Technology", Proceedings, 6th Symposium on Computer Arithmetic (IEEE), (1983), 10-16	
		SCHMOOKLER, M. S., et al., "Group-Carry Generator", IBM Technical Disclosure Bulletin, 6(1), (June, 1963), 77-78	
		SKLANSKY, J., "Conditional-Sum Addition Logic", IRE Trans., EC-9, (June 1960), 226-231	
		SWARTZLANDER, JR., E. E., "Parallel Counters", IEEE Transactions on Computers, C-22(11), (November 1973), 1021-1024	
		TSAI, W.-C., et al., "Two Systolic Architectures for Modular Multiplication", IEEE Transactions on VLSI Systems, Vol. 8(1), (2000), 103-107	
		VASSILIADIS, S., et al., "7/2 Counters and Multiplication with Threshold Logic", IEEE, (1997), 192-196	
		WEINBERGER, A., et al., "A Logic for High-Speed Addition", Nat. Bur. Stand. Circ., 591, (1958), 3-12	
		WEINBERGER, A., "Extension of the Size of Group Carry Signals", IBM Technical Disclosure Bulletin, 22(4), (September, 1979), 1548-1550	
		WEINBERGER, A., "Improved Carry-Look-Ahead", IBM Technical Disclosure Bulletin, 21(6), (November, 1978), 2460-2461	
		ZURAS, D., et al., "Balanced delay trees and combinatorial division in VLSI", IEEE Journal of Solid State Circuits, SC-21(5), (1986),814-819	

EXAMINER **DATE CONSIDERED**

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional) [2] Applicant is to place a check mark here if English language Translation is attached